Published and Copyright (c) 1999 - 2012
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1418 05/11/12

~ US, China To Cooperate! ~ People Are Talking! ~ Win 8 Restrictions!
~ New Xbox in Production? ~ Oracle Guilty in Trial! ~ McAfee Is Persecuted?

~ Sega Urine-Powered Game! ~ Spy Agency Can Keep Mum ~ FBI Needs Web Wiretap!

~ Facebook Data Use Policy ~ ~ Xbox 360 With Kinect!

-* New $99 Xbox With A Catch! *-
-* FBI Wants Easier Web Surveillance! *-
-* Oracle's Fair Use Request Ruling Denied! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Things are still hectic around here, as you could imagine. Very little time to ourselves these days, much less much time for "extra-curricular" activities. This week's issue has been put together quite quickly; and a number of articles in this issue kindly submitted by longtime reader Fred Horvat. Fred continues to "feed" me article ideas on a weekly basis; and I really appreciate the aid - especially these days when I don't have as much time as I'd like.

So, let's move on to the issue - that's the real reason we're here anyway!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Next Xbox Already in Production?
""""""""""""""""""""""""""""""""" $99 Xbox Consoles With A Catch!
Sega Vidro Game, Powered by Urine!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Next Xbox May Already Be in Production

A Texas electronics company has allegedly begun production on Microsoft s next-generation Xbox gaming console, according to a report from IGN. Production of the Xbox 720 is reportedly underway at the Austin, Texas

branch of Flextronics, the same electronics company responsible for manufacturing the Xbox 360 and the original Xbox. Despite these reports, however, Microsoft firmly stated that the next-generation Xbox will not debut at this year s E3 gaming convention. The hardware currently being manufactured may instead be development kits for top-tier game developers that will get early access to Microsoft s next-generation hardware in order to prepare new titles. The Xbox 720" is rumored to be six times more powerful than the current Xbox. It has been reported that the console will be equipped with a GPU based on ATI s Radeon HD 6670 and should offer support for 3D technology, 1080p HD output, multiple displays and DirectX 11. Microsoft may also be looking to use online downloads and swappable solid state cards rather than a traditional disc drive.

Microsoft Offers $99 Xbox Consoles With A Catch

Microsoft on Monday began testing whether a pricing strategy that has been a hit with smartphones will invigorate sales of its Xbox 360 videogame consoles.

The technology titan began offering four-gigabyte consoles bundled with Kinect voice-and-gesture sensing controllers at select Microsoft stores in the United States for $99.

The catch is that buyers must subscribe for two years to the Xbox Live Gold online service for games, films, music and play. The monthly subscription fee was $15, bringing the total cost to about $460 over time.

Paying for the console, Kinect, and Live memberships up front at prices advertised online Monday indicated that buyers would break even or perhaps save as much as $40 by paying up front.

The tactic of subsidizing hardware with an eye toward profiting in the long run has served telecom carriers well when it comes to smartphone buyers who snap up handsets at heavy discounts but lock into contracts for service.

Microsoft said in its quarterly earnings report last month that market-leading sales of Xbox consoles had softened.

Money taken in by the company’s Entertainment and Devices Division that had been ablaze due to Xbox and its Kinect accessory dropped 16 percent to $1.6 billion in the recently ended quarter.

Xbox 360 with Kinect Controls

Microsoft is currently testing a modified version of Internet Explorer 9 on its Xbox 360 console, according to our sources. The Xbox 360 currently includes Bing voice search, but it’s limited to media results. Microsoft’s new Internet Explorer browser for Xbox will expand on this functionality to open up a full browser for the console. We are told that the browser will let Xbox users surf all parts of the web straight from their living rooms.

Microsoft has also integrated Kinect gestures and voice control heavily into the experience, allowing Xbox owners to quickly search using the existing Bing functionality and pull up relevant web pages. Kinect support is not mandatory according to our sources, but the browser is said to be tuned for Kinect usage. There's no word on a launch date for Internet Explorer on Xbox, but with E3 on the horizon we'd expect to hear the official details from Microsoft in a matter of weeks.

Sega Launches A New Video Game Powered by Urine

Sega exited the video game console business in 2001 after stiff competition from Microsoft, Sony and Nintendo forced the struggling company to shift gears. Now, more than 10 years later, Sega is back with new video game hardware but it s definitely not the kind you might expect. Unveiled late last year, Sega s Toylet is now available in Japan and the surrounding region. The system connects to a urinal, allowing users to play a variety of interactive games by urinating on a sensor connected to the main device. A screen above the system then displays each game to the player, examples of which include filling virtual coffee cans and blowing wind up a cartoon news anchor s dress. The Toylet costs roughly $1,750 and each game runs an additional $125, but it s likely money well spent for bar owners, at least until the novelty wears off. A video demo of the Toylet (not in action, thankfully) follows below along with a pair of images that show examples of Toylet installations in Tokyo.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

US, China To Cooperate More on Cyber Threat

Asserting that cyberattacks against the U.S. don't come only from China, the U.S. and Chinese defense ministers said they agreed Monday to work together on cyber issues to avoid miscalculations that could lead to future crises.

Defense Secretary Leon Panetta said that since China and the United States have advanced cyber capabilities, it is important to develop better cooperation.

"It's true, as the general pointed out, that obviously there are other countries, actors, others involved in some of the attacks that both of our countries receive," Panetta told reporters after an afternoon meeting in the Pentagon marking the first visit by a Chinese defense minister to the U.S. since 2003. "But because the United States and China have developed technological capabilities in this arena it's extremely important that we work together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area."

Gen. Liang Guanglie, China’s minister of national defense, offered a vigorous defense of his country, saying through an interpreter that, "I can hardly agree with the proposition that the cyberattacks directed to the United States are directly coming from China. ... We cannot attribute all of the cyberattacks (against the) United States to China."

Just six months ago, however, senior U.S. intelligence officials for the first time publicly accused China of systematically stealing American high-tech data for its own national economic gain.

It was the most forceful and detailed airing of U.S. allegations against Beijing after years of private complaints, and it signaled the opening salvo of a broad diplomatic push to combat cyberattacks that originate in China.

Liang said that he and Panetta talked about ways to strengthen cybersecurity, but they are leaving the details to the experts.

Cybersecurity was just one of the many issues discussed by the two leaders during their meeting, but it is also one of a number of contentious topics that rattle the often rocky relationship between the two nations.

"The U.S. needs to start laying the ground work for better understanding by the Chinese of what we expect from them in cyberspace," said James Lewis, a cybersecurity expert with the Center for Strategic and International Studies who has met with Chinese officials and scholars for informal discussions. "We want to figure out some way to get some understanding in place before something bad happens."

As an example he said American officials want to know who to talk to when Chinese hackers breach U.S. computer networks. And if there is a cyber incident in China, Lewis said, "we need the Chinese to feel confident that they can call us up and ask, ’was it you?’, and get a straight answer."

Chinese officials have routinely denied the cyberspying, insisting that their own country also is a victim of such attacks. And they note that the hacking is anonymous and often difficult to track.

U.S. cybersecurity experts acknowledge that attribution can be difficult, and that while they can trace an attack to China, it is often difficult to track directly to the Chinese government. Last December’s report by U.S. intelligence agencies said America must openly confront China and Russia in a broad diplomatic push to combat cyberattacks that are on the rise and represent a "persistent threat to U.S. economic security."

And, separately, several cybersecurity analysts have concluded that as few as 12 different Chinese groups, largely backed or directed by the government there, commit the bulk of the cyberattacks that aim to steal critical data from U.S. companies and government agencies. Officials estimate that the stealthy attacks have stolen billions of dollars in intellectual property and data.

Because people and businesses in both China and American have been victims of cyberattacks, officials have been talking more about building a better relationship so that they can work together.

Law enforcement is one area of cybersecurity where the two nations have begun to build partnerships, but so far it has been extremely limited. Lewis said that in 2011, U.S. authorities requested assistance from the

Chinese 11 times, and in seven of the cases received no information. But, he said the Chinese cooperated with U.S. law enforcement in a high profile financial fraud case late last year.

FBI Wants Easier Internet Surveillance, Seeks Nod From Web Companies

The FBI is waging a charm offensive to persuade Internet companies not to oppose a proposal to require that e-mail and networking tools be built with backdoors to allow government surveillance, CNET has reported.

The move suggests the agency is finding it difficult to intercept Internet communications as Web applications get increasingly complex.

The FBI general counsel's office has drafted a proposed law to require social-media sites, e-mail providers, and voice over Internet protocol services - such as Skype - to adjust their source code to allow the government to listen in on traffic, according to the report. It would expand the Communications Assistance for Law Enforcement Act, which requires that telecommunications providers -- but not Web companies - build their systems to be wiretap-friendly.

The FBI is in talks with Web companies on how it can implement this rule and minimize its costs to the industry.

A growing gap exists between the statutory authority of law enforcement to intercept electronic communications pursuant to court order and our practical ability to intercept those communications, an agency representative told CNET. The FBI believes that if this gap continues to grow, there is a very real risk of the government 'going dark,' resulting in an increased risk to national security and public safety."

FBI: We Need Wiretap-Ready Web Sites - Now

The FBI is asking Internet companies not to oppose a controversial proposal that would require firms, including Microsoft, Facebook, Yahoo, and Google, to build in backdoors for government surveillance.

In meetings with industry representatives, the White House, and U.S. senators, senior FBI officials argue the dramatic shift i communication from the telephone system to the Internet has made it far more difficult for agents to wiretap Americans suspected of illegal activities, CNET has learned.

The FBI general counsel's office has drafted a proposed law that the bureau claims is the best solution: requiring that social-networking Web sites and providers of VoIP, instant messaging, and Web e-mail alter their code to ensure their products are wiretap-friendly.

"If you create a service, product, or app that allows a user to communicate, you get the privilege of adding that extra coding," an industry representative who has reviewed the FBI's draft legislation told CNET. The requirements apply only if a threshold of a certain number of users is exceeded, according to a second industry representative briefed on it.

The FBI’s proposal would amend a 1994 law, called the Communications Assistance for Law Enforcement Act, or CALEA, that currently applies only to telecommunications providers, not Web companies. The Federal Communications Commission extended CALEA in 2004 to apply to broadband networks.

June 2008: FBI Director Robert Mueller and his aides brief Sens. Barbara Mikulski, Richard Shelby, and Ted Stevens on "Going Dark."

June 2008: FBI Assistant Director Kerry Haynes holds "Going Dark" briefing for Senate appropriations subcommittee and offers a "classified version of this briefing" at Quantico.

August 2008: Mueller briefed on Going Dark at strategy meeting.

September 2008: FBI completes a "high-level explanation" of CALEA amendment package.

May 2009: FBI Assistant Director Rich Haley briefs Senate Intelligence committee and Mikulsi staffers on how bureau is "dealing with the ’Going Dark’ issue.’" Mikulski plans to bring up "Going Dark" at a closed-door hearing the following week.

May 2009: Haley briefs Rep. Dutch Ruppersberger, currently the top Democrat on House Intelligence, who would later co-author CISPA.

September 2008: FBI staff briefed by RAND, which was commissioned to "look at" Going Dark.

November 2008: FBI Assistant Director Marcus Thomas, who oversees the Quantico-based Operational Technology Division, prepares briefing for President-Elect Obama’s transition team.

December 2008: FBI intelligence analyst in Communications Analysis Unit begins analysis of VoIP surveillance.

February 2009: FBI memo to all field offices asks for anecdotal information about cases where "investigations have been negatively impacted" by lack of data retention or Internet interception.

March 2009: Mueller’s advisory board meets for a full-day briefing on Going Dark.

April 2009: FBI distributes presentation for White House meeting on Going Dark.

April 2009: FBI warns that the Going Dark project is "yellow," meaning limited progress, because of "new administration personnel not being in place for briefings."

April 2009: FBI general counsel’s office reports that the bureau’s Data Interception Technology Unit has "compiled a list of FISA dockets... that the FBI has been unable to fully implement." That’s a reference to telecom companies that are already covered by the FCC’s expansion of CALEA.

May 2009: FBI’s internal Wikipedia-knockoff Bureaupedia entry for "National Lawful Intercept Strategy" includes section on "modernize lawful intercept laws."

May 2009: FBI e-mail boasts that the bureau's plan has "gotten attention" from industry, but "we need to strengthen the business case on this."

June 2009: FBI's Office of Congressional Affairs prepares Going Dark briefing for closed-door session of Senate Appropriations subcommittee.

July 2010: FBI e-mail says the "Going Dark Working Group (GDWG) continues to ask for examples from Cvber investigations where investigators have had problems" because of new technologies.

September 2010: FBI staff operations specialist in its Counterterrorism Division sends e-mail on difficulties in "obtaining information from Internet Service Providers and social-networking sites."

FBI Director Robert Mueller is not asking companies to support the bureau's CALEA expansion, but instead is "asking what can go in it to minimize impacts," one participant in the discussions says. That included a scheduled trip this month to the West Coast - which was subsequently postponed - to meet with Internet companies' CEOs and top lawyers.

A further expansion of CALEA is unlikely to be applauded by tech companies, their customers, or privacy groups. Apple (which distributes iChat and FaceTime) is currently lobbying on the topic, according to disclosure documents filed with Congress two weeks ago. Microsoft (which owns Skype and Hotmail) says its lobbyists are following the topic because it's "an area of ongoing interest to us." Google, Yahoo, and Facebook declined to comment.

In February 2011, CNET was the first to report that then-FBI general counsel Valerie Caproni was planning to warn Congress of what the bureau calls its "Going Dark" problem, meaning that its surveillance capabilities may diminish as technology advances. Caproni singled out "Web-based e-mail, social-networking sites, and peer-to-peer communications" as problems that have left the FBI "increasingly unable" to conduct the same kind of wiretapping it could in the past.

In addition to the FBI's legislative proposal, there are indications that the Federal Communications Commission is considering reinterpreting CALEA to demand that products that allow video or voice chat over the Internet - from Skype to Google Hangouts to Xbox Live - include surveillance backdoors to help the FBI with its "Going Dark" program. CALEA applies to technologies that are a "substantial replacement" for the telephone system.

"We have noticed a massive uptick in the amount of FCC CALEA inquiries and enforcement proceedings within the last year, most of which are intended to address 'Going Dark' issues," says Christopher Canter, lead compliance counsel at the Marashlian and Donahue law firm, which specializes in CALEA. "This generally means that the FCC is laying the groundwork for regulatory action."

Subsentio, a Colorado-based company that sells CALEA compliance products and worked with the Justice Department when it asked the FCC to extend CALEA seven years ago, says the FBI's draft legislation was prepared with the compliance costs of Internet companies in mind.

In a statement to CNET, Subsentio President Steve Bock said that the measure provides a "safe harbor" for Internet companies as long as the

interception techniques are "'good enough' solutions approved by the attorney general."

Another option that would be permitted, Bock said, is if companies "supply the government with proprietary information to decode information" obtained through a wiretap or other type of lawful interception, rather than "provide a complex system for converting the information into an industry standard format."

A representative for the FBI told CNET today that: "(There are) significant challenges posed to the FBI in the accomplishment of our diverse mission. These include those that result from the advent of rapidly changing technology. A growing gap exists between the statutory authority of law enforcement to intercept electronic communications pursuant to court order and our practical ability to intercept those communications. The FBI believes that if this gap continues to grow, there is a very real risk of the government 'going dark,' resulting in an increased risk to national security and public safety."

The FBI's legislation, which has been approved by the Department of Justice, is one component of what the bureau has internally called the "National Electronic Surveillance Strategy." Documents obtained by the Electronic Frontier Foundation show that since 2006, Going Dark has been a worry inside the bureau, which employed 107 full-time equivalent people on the project as of 2009, commissioned a RAND study, and sought extensive technical input from the bureau's secretive Operational Technology Division in Quantico, Va. The division boasts of developing the "latest and greatest investigative technologies to catch terrorists and criminals."

But the White House, perhaps less inclined than the bureau to initiate what would likely be a bruising privacy battle, has not sent the FBI's CALEA amendments to Capitol Hill, even though they were expected last year. (A representative for Sen. Patrick Leahy, head of the Judiciary committee and original author of CALEA, said today that "we have not seen any proposals from the administration.")

Mueller said in December that the CALEA amendments will be "coordinated through the interagency process," meaning they would need to receive administration-wide approval.

Stewart Baker, a partner at Steptoe and Johnson who is the former assistant secretary for policy at Homeland Security, said the FBI has "faced difficulty getting its legislative proposals through an administration staffed in large part by people who lived through the CALEA and crypto fights of the Clinton administration, and who are jaundiced about law enforcement regulation of technology - overly jaundiced, in my view."

On the other hand, as a senator in the 1990s, Vice President Joe Biden introduced a bill at the FBI's behest that echoes the bureau's proposal today. Biden's bill said companies should "ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law." (Biden's legislation spurred the public release of PGP, one of the first easy-to-use encryption utilities.)

The Justice Department did not respond to a request for comment. An FCC representative referred questions to the Public Safety and Homeland Security Bureau, which declined to comment.

From the FBI’s perspective, expanding CALEA to cover VoIP, Web e-mail, and social networks isn’t expanding wiretapping law: If a court order is required today, one will be required tomorrow as well. Rather, it’s making sure that a wiretap is guaranteed to produce results.

But that nuanced argument could prove radioactive among an Internet community already skeptical of government efforts in the wake of protests over the Stop Online Piracy Act, or SOPA, in January, and the CISPA data-sharing bill last month. And even if startups or hobbyist projects are exempted if they stay below the user threshold, it’s hardly clear how open-source or free software projects such as Linphone, KPhone, and Zfone - or Nicholas Merrill’s proposal for a privacy-protective Internet provider - will comply.

The FBI’s CALEA amendments could be particularly troublesome for Zfone. Phil Zimmermann, the creator of PGP who became a privacy icon two decades ago after being threatened with criminal prosecution, announced Zfone in 2005 as a way to protect the privacy of VoIP users. Zfone scrambles the entire conversation from end to end.

"I worry about the government mandating backdoors into these kinds of communications," says Jennifer Lynch, an attorney at the San Francisco-based Electronic Frontier Foundation, which has obtained documents from the FBI relating to its proposed expansion of CALEA.

As CNET was the first to report in 2003, representatives of the FBI’s Electronic Surveillance Technology Section in Chantilly, Va., began quietly lobbying the FCC to force broadband providers to provide more-efficient, standardized surveillance facilities. The FCC approved that requirement a year later, sweeping in Internet phone companies that tie into the existing telecommunications system. It was upheld in 2006 by a federal appeals court.

But the FCC never granted the FBI’s request to rewrite CALEA to cover instant messaging and VoIP programs that are not "managed"--meaning peer-to-peer programs like Apple’s Facetime, iChat/AIM, Gmail’s video chat, and Xbox Live’s in-game chat that do not use the public telephone network.

If there is going to be a CALEA rewrite, "industry would like to see any new legislation include some protections against disclosure of any trade secrets or other confidential information that might be shared with law enforcement, so that they are not released, for example, during open court proceedings," says Roszel Thomsen, a partner at Thomsen and Burke who represents technology companies and is a member of an FBI study group. He suggests that such language would make it "somewhat easier" for both industry and the police to respond to new technologies.

But industry groups aren’t necessarily going to roll over without a fight. TechAmerica, a trade association that includes representatives of HP, eBay, IBM, Qualcomm, and other tech companies on its board of directors, has been lobbying against a CALEA expansion. Such a law would "represent a sea change in government surveillance law, imposing significant compliance costs on both traditional (think local exchange carriers) and nontraditional (think social media) communications companies," TechAmerica said in e-mail today.

Ross Schulman, public policy and regulatory counsel at the Computer and Communications Industry Association, adds: "New methods of communication should not be subject to a government green light before they can be

used."

Oracle’s Request for Fair Use Ruling Denied

Following the jury’s inability to decide on the issue of fair use in the Oracle vs. Google trial, Oracle asked the judge to rule on the issue as a matter of law (JMOL). Both sides engaged in oral arguments, but Judge William Alsup surprised the courtroom with an early decision, denying Oracle’s request, saying that "it wouldn’t be fair" given the evidence introduced in the trial.

While the jury found that Google had infringed upon Oracle’s copyrights by using the sequence, structure, and organization (SSO) of the 37 Java APIs in question, it was deadlocked on whether Google was legally able to do so under fair use. Fair use is made up of four different components:

The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes
The nature of the copyrighted work
The amount and substantiality of the portion used in relation to the copyrighted work as a whole
The effect of the use upon the potential market for, or value of, the copyrighted work

The elements are taken as a whole, with no single one making or breaking the decision; it’s a balancing act. However, despite Oracle pointing out the commercial success of Android — which would tend to weigh against a finding of fair use — it was clear that Judge Alsup wasn’t inclined to side with the company. The judge even scolded Oracle counsel Michael Jacobs when he first argued his case, pointing out that the company’s legal team had insisted on a jury trial and "now we got their verdict and you want something else."

"The judge could make things even worse for Oracle"

As for what’s next, there’s still much on the copyright side to be decided. The judge has yet to rule on Google’s motion for a mistrial — something that became a little more likely today — and he has yet to decide on the overall copyrightability of the structure, sequence, and organization of the 37 Java APIs themselves. Ruling that the APIs are not covered would render today’s decision meaningless, essentially throwing away the jury’s earlier finding of infringement on the SSO issue. Judge Alsup said that if another trial does indeed end up being required — something he seemed loath to even consider — a better way to proceed would be to decide what portions can be copyrighted, and then determine fair use from there. Given the jury’s indecision, this could end up being the best way to reach a decision if the case is retried (of course, several of the decisions and issues in the last few weeks will likely result in an appeal).

As for Google, after weeks of legal battle the company is now left facing just one count of infringement: the nine lines of rangeCheck code found in TimSort.java and ComparableTimSort.java. Google could have been found to have infringed on a total of five different counts; now it’s been reduced to just the one, and with rangeCheck constituting such a small portion of Android’s 15 million lines of code, any potential damages coming Oracle’s way will likely be very small indeed. Of course, we’re

still in the thick of the patent phase of the trial, with the damages portion to follow. We'll be there to bring you the latest.

Google Guilty of Infringement in Oracle Trial; Future Legal Headaches Loom

In what could be a major blow to Android, Google's mobile operating system, a San Francisco jury issued a verdict today that the company broke copyright laws when it used Java APIs to design the system. The ruling is a partial victory for Oracle, which accused Google of violating copyright law.

But the jury couldn't reach agreement on a second issue whether Google had a valid "fair use" defense when it used the APIs. Google has asked for a mistrial based on the incomplete verdict, and that issue will be briefed later this week.

The results aren't clear going forward. Both sides are going to write briefs arguing how to proceed from here, with Google likely arguing the verdict needs to be thrown out, while Oracle somehow tries to hang on to its win on question 1A, the fundamental question about whether Google infringed copyright.

No one knows the jury's internal deliberations, so it's speculative to guess at what led to the partial verdict. But one reason could be the unusual construction of this trial. Judge William Alsup, who is overseeing the case, ruled that the case would be decided by a jury of 12, which is large for a civil case and increases the possibility of having one or more "holdout" jurors. Alsup also ruled that the jury must decide unanimously, a requirement for criminal cases that's not always imposed on civil juries.

On two other questions whether Google violated copyrights on certain software documentation, and a question about whether Google's acknowledged copying of a few short software functions also broke copyright laws the jury found mostly in Google's favor. There was no infringement found regarding the documentation, but the jury did find that one nine-line function that Google acknowledged copying was infringing. (If that's all that holds up, though, there won't be much in way of damages available to Oracle.)

What is clear is that the jury believes that Google did copy something important. Even though Google's code in Android was original or borrowed from other open source code, the jury found that the Android APIs copied the "structure, sequence, and organization" of Java APIs.

Google spokesman Jim Prosser responded to the verdict quickly, saying via e-mail: "We appreciate the jury's efforts, and know that fair use and infringement are two sides of the same coin. The core issue is whether the APIs here are copyrightable, and that's for the court to decide. We expect to prevail on this issue and Oracle's other claims."

If the verdict stands, the end result is that Java may not be as open source as it was thought to be. Oracle may be able to essentially take Java out of the public domain, at least as far as its use in cell phones.

Oracle may have a leg up in the patent phase. It's already managed to sway these 12 jurors on the key question, and the same panel is now considering

Oracle’s allegations that Google has infringed two Java-related patents.

This is far from being a loss for Google at this point, however. Even if it doesn’t manage to get Judge Alsup to declare a mistrial, the search giant has other ways it could avoid a big copyright loss.

First of all, Alsup let the jury trial move forward without making a key ruling: whether APIs are copyrightable at all. Instead, he let the evidence develop throughout the trial, and told the jury to assume that APIs can be copyrighted. But at the end of the trial, Alsup gave the lawyers a short talk indicating that he may see the API issue Google’s way, comparing APIs to an idea for writing a guide book from San Francisco to Monterey.

If the verdict that Android infringed copyrights stands, it could put programmers in a difficult situation. Java is an open source language, but now it’s not clear how free programmers are to use it, since Oracle has said that anyone following the Java APIs which are basically sets of instructions about how to use Java needs a license.

The effects beyond Android and Java are unclear. At this point, Android is the only "non-standard" implementation of Java. However, it could have a chilling effect, and if Oracle is seen as a major IP enforcer when it comes to Java, that could backfire.

"Other people will be deterred from using Java as the basis for some non-standard thing in the future," said Tyler Ochoa, a professor of copyright law at Santa Clara University. "It could be the case that Oracle wins the battle and loses the war."

For all that, Oracle won today on the key question. The company’s long battle to get money out of Google and Android is looking like it stands a much better chance today. While Oracle is a large company with many operations and hardly a "patent troll," in a way, it may be able to execute a similar strategy getting a cut of the lucrative smartphone market using intellectual property laws, even though it doesn’t compete in that market. What kind of money Oracle will be able to collect will be determined in a third "damages phase" of the trial. That phase will start after the "patent phase," which begins today and may only last one week.

Overall, the situation bodes poorly for Google’s legal defense of Android, which will be ongoing. Oracle’s lawsuit was the most aggressive and well-funded of many intellectual property attacks against Android. But Google will continue to be involved in Android-related patent litigation, as the handset companies that make Android phones, like Samsung and HTC, are being sued by Microsoft and Apple in a kind of "proxy war" against Android.

Despite these legal attacks, Android is experiencing explosive growth; a Google executive testified last week that 750,000 Android phones are being activated each day in 2012. That’s up from 160,000 per day in 2010.

After the partial copyright verdict was read, Judge Alsup launched right into the patent phase without even giving a break. Right now, the jury is watching a video about patents and patent lawsuits produced by the Federal Judicial Center, which is commonly shown to patent juries. Court will probably adjourn after opening statements today, and witnesses will begin testifying tomorrow, possibly including a repeat show by Jonathan Schwartz, the ex-Sun CEO. The patent phase is expected to be concluded

in as little as one week.

US Spy Agency Can Keep Mum on Google Ties

The top-secret US National Security Agency is not required to reveal any deal it may have with Google to help protect against cyber attacks, an appeals court ruled Friday.

The US Court of Appeals in Washington upheld a lower court decision that said the NSA need not confirm or deny any relationship with Google, because its governing statutes allow it keep such information secret.

The ruling came in response to a Freedom of Information Act request from a public interest group, which said the public has a right to know about any spying on citizens.

The appeals court agreed that the NSA can reject the request, and does not even have to confirm whether it has any arrangement with the Internet giant.

"Any information pertaining to the relationship between Google and NSA would reveal protected information about NSA’s implementation of its information assurance mission," Judge Janice Rogers Brown wrote in the appeals opinion.

The non-profit Electronic Privacy Information Center (EPIC) filed a formal request to make public documents related to the dealings, and said much of the information had already been in news media.

The request stemmed from a January 2010 cyber attack on Google that primarily targeted the Gmail email accounts of Chinese human rights activists.

According to the Google blog, the Internet group’s chief legal officer David Drummond stated that the firm was notifying other companies that may have been targeted and was also working with the relevant US authorities.

The Wall Street Journal and Washington Post reported that Google had contacted the NSA immediately following the attack.

According to news reports, the NSA agreed to help Google analyze the attacks in a bid to better protect the California-based search company and its users from future intrusions.

The reported alliance would seek to allow the spy agency to evaluate Google’s hardware and software vulnerabilities, as well as estimate the sophistication of its adversary in order to help the firm understand whether it has the right defenses in place.

Privacy advocates already critical of Google policies regarding saving user data and targeting ads to match online behavior patterns fear that an alliance with the spy network could put private information at risk.

Facebook Updates Data Use Policy To Give More Info

Facebook is updating its data use policy in an attempt to give people more clarity on how the company uses information they share.

As part of the changes, Facebook is also signaling that it may start showing people ads on sites other than Facebook, targeting the pitches to interests and hobbies that users express on Facebook.

The move comes a week before Facebook Inc.’s expected initial public offering of stock. Facebook held events with potential investors this week, including one in Silicon Valley on Friday, and it has posted a version of its road show online. The offering could value Facebook at nearly $100 billion more than Kraft, Ford and other major brands.

The policy changes are in response to an audit by Irish data-protection authorities last year, Facebook said Friday. The commission had asked Facebook to be more transparent about how it collects people’s data and uses it for advertising, as well as how long it keeps such information.

Facebook plans to notify its more than 900 million users of the changes through advertisements around the site and on its mobile apps. Users who want to dig deeper can read a version of the policy that highlights the changes word by word. Erin Egan, Facebook’s chief privacy officer, will host an online chat Monday to answer any questions.

Egan said the company wasn’t substantially changing its business practices, but wants to "err on the side of providing too much information."

Facebook’s overseas headquarters are based in Dublin, Ireland, a member of the European Union. This means the company is required to comply with European data privacy laws. Facebook said the changes were also a response to feedback from its users.

As part of the changes to the policy, Facebook has created a section to explain how it uses technologies such as cookies to deliver ads, secure the site and offer various features. Cookies, which are small files containing data or alphanumeric IDs, are commonly used to track people’s activities around the Web, for example. The information could then be used to target ads to their hobbies and interests.

The changes also incorporate updates that Facebook has made to its site since its previous policy revision announced in September. This includes reorganizing people’s profile pages in a "timeline" format and adding an "activity log" that lets people see everything they’ve done on the site, as well as who can see it. The "cover photo" people put on their timeline is considered public information, along with their gender.

Facebook also has given itself more leeway on how long it keeps information it collects. Before, it has typically kept such data for 180 days. Facebook said it will now retain data for "as long as it is necessary to provide services." This could be longer or shorter than 180 days.

For example, if a company creates a "page" for its brand, Facebook said it wouldn’t delete the information put there "simply because 180 days had passed."

"Instead, we would delete it when it was no longer needed when the page

owner deleted it or closed its account," Facebook said.

Some of the changes give a glimpse of what Facebook might do in the future. Though it doesn't currently show people ads outside of Facebook.com or its mobile apps, the updated policy gives it the option to do so. This is something other companies, such as Amazon.com Inc.'s Zappos.com, already do. For example, people who click on shoes while shopping on Zappos might see the same shoes pop up in ads elsewhere, even if they are not logged into Zappos. This is what cookies do.

Justin Brookman, director of consumer privacy at the nonprofit Center for Democracy and Technology, said Facebook hasn't been very explicit about this possibility before, "but now they seem to be calling it out."

While such ads may "creep people out," he added, it doesn't mean the company would be collecting more information about users than it already does. It's also a new revenue source.

Jules Polonetsky, director of the Future of Privacy Forum, an industry-backed think tank in Washington, said Facebook's overall data use policy is "a really interesting document" that teaches users how the service works sort of like a user's guide.

Most privacy policies read like legal documents, though there are other exceptions, such as Google Inc.

Still, he added, it's a "very small audience that takes the time to read even the most delightful and entertaining privacy policy."

What's more useful, Polonetsky said, is to give users advice and options at the time that they need the information. Facebook already does this in many cases. For example, when users post a status update, they can decide whether that will be visible to their friends or to the broader public.

"That's how people are really going to learn," he said.

Mozilla, Google Voice Concern over Windows 8 Browser Restrictions

Both Mozilla and Google have expressed concern over Windows 8. Microsoft's next big operating system release restricts access to certain APIs and technologies browsers need - only making them available to Internet Explorer. Looking at the facts, it would seem Mozilla and Google have a solid case - coincidentally, the responses on the web are proof of the slippery slope we're on regarding ownership over our own machines.

It's important to make a distinction between Windows 8 on ARM (Windows RT) and regular Windows. Mike Pall, developer of, among other things, a just-in-time compiler for Lua, explains what, exactly, browser developers do not have access to on Windows 8 on ARM. First, it's important to know that even though Windows RT ships with the Win32 APIs installed, only Microsoft can access them - which it does for Office 15 and Internet Explorer. Third party developer do not have access to Win32; they can only access the WinRT APIs.

The WinRT API does not offer the equivalent of VirtualAlloc() or VirtualProtect() with the ability to make code executable at runtime. But JIT compilers absolutely require this functionality, which means there'll

be NO INDEPENDENT JIT COMPILERS for W8ARM!" Pall explains, "The Internet Explorer process on W8ARM has special privileges and is the only one allowed to run a JIT compiler to speed up JavaScript. No other browser will be able to compete on performance with IE on W8ARM. That sure simplifies keeping up with the competition..."

"Actually, fully-functional browsers need access to a couple more APIs that is denied to them, too. But the inability to run a JIT compiler has consequences for a much wider range of software," he adds, "For W8ARM there'll be no LuaJIT (in JIT mode), no PyPy, no Java, no v8, just to name a few. Ditto for any software that relies on them (Scala, Clojure, JRuby) or embeds them."

These same restrictions apply to Windows 8 on x86, but only for Marketplace applications. Contrary to Windows 8 on ARM, you can still install your own desktop applications on Windows 8 x86, including a special class of applications which combine the Win32 API with WinRT. In any case, it's pretty obvious the desktop is legacy, so it'll eventually be phased out.

These are some pretty hefty limitations, and considering Internet Explorer on Windows 8 doesn't have to respect these limitations, it's clear it will have a considerable advantage over possible competing solutions. Rightfully so, Mozilla and Google are not particularly happy about this.

"The prospect that the next generation of Windows on ARM devices would limit users to one browser is untenable and represents a first step toward a new platform lock-in," writes Harvey Anderson, Mozilla general counsel.

Asa Dotzler further adds that this goess well beyond tablets alone. "ARM will be migrating to laptop PCs and all-in-one PCs very quickly. If you read Microsoft's blog posts about Windows on ARM, you'll see that they expect ARM PCs to cover the whole spectrum. ARM chips are already being used in servers. This is not a tablet-only concern," he argues.

I agree with Dotzler - heck, the one reason I'm excited about Windows on ARM is that it will finally be interesting for big OEMs to start shipping laptops and desktops with ARM chips in them. Considering I don't give a rat's bum about gaming or things like photo or video editing, I'd love a super-small, silent, and frugal ARM box which I can tape to the back of my monitor, running Windows (yes, I prefer Windows over Linux and Mac OS X - sue me).

However, I'm not particularly enamoured with Internet Explorer as it exists on the preview versions of Windows 8 (for various reasons I won't go into), and I'd love for, say, Google to make a WebKit Metro browser I actually like. The current limitations make that entirely impossible, which sucks.

Speaking of Google, it, too, has raised concerns over the browser situation on Windows 8. "We share the concerns Mozilla has raised regarding the Windows 8 environment restricting user choice and innovation," the company told Cnet, "We've always welcomed innovation in the browser space across all platforms and strongly believe that having great competitors makes us all work harder. In the end, consumers and developers benefit the most from robust competition."

Most responses online have focussed on the fact that Windows RT is supposed to focus on tablets (which isn't true, as Dotzler pointed out, but alas), and as such, the situation isn't much different from iOS. As a

geek, this line of reasoning saddens me greatly - it confirms just how out of touch the industry has become with its roots. It’s the slippery slope many warned about: now that iOS is successful, we’ve already accepted that we no longer get to decide what code we get to run on our own devices, so much so that even Microsoft can get away with limiting us in this fashion. Mac OS X is moving in the same direction.

I’m quite young (born in 1984, ironically enough), but even I learned about computers the hard way - by messing stuff up. By breaking stuff. By stepping outside of the boundaries set by my parents and school regarding computer use. By age 6 or 7 I was hooked enough to start dabbling with BASIC - which wouldn’t be possible in a Metro and iOS world. This is something that honestly and truly has me worried, because 10-20 years from now, we’re still going to need great programmers, and if all they know are the nanny states of Metro and iOS, we’re going to be in for a nasty surprise.

Let me be very harsh and make it very clear: I’m not talking about people who write a bunch of iOS applications and call it a day. I’m talking about the nitty gritty stuff. Driver development. Assembly programming. Kernel development. Firmware stuff.

Let me extend an olive branch for once and assume that Microsoft and Apple are doing this for entirely altruistic reasons - under that assumption, this is a well-intentioned but entirely dangerous development that we shouldn’t cheer on, but be weary of. It’d be such a huge step in the right direction if they were to, I don’t know, commit to implementing a sideloading switch for the foreseeable future.

All in all, this is a major issue, and I don’t buy into the whole "it has no keyboard so it shouldn’t be your device"-nonsense. If it takes the government or the justice system to step in and resolve this, then, well... So be it.

McAfee Founder Claims Persecution in Belize

The founder of the computer virus software company McAfee, Inc. says he is being persecuted by police in his home in the Central American country of Belize.

John McAfee told The Associated Press that officers from the country’s Gang Suppression Unit raided his home late last month in what they called a search for illegal drugs and ammunition. McAfee said he is being punished for refusing to donate money to a local politician.

Police on Monday declined a request to comment.

McAfee told the AP on Friday that he was leaving his home and turning off his cell phone in order to hide in an undisclosed location because he was afraid for his safety. He could not be reached for further comment.

McAfee told The New York Times in 2009 that he had lost all but $4 million of his $100 million in the U.S. financial crisis, and was moving to Belize in order to pay less taxes. He sold his stake in the anti-virus company in the early 90s.

He said that police who raided his gated home in the town of Orange Walk

handcuffed his employees and held them for hours before releasing them without charge. He says he had weapons in his compound, including a 9mm pistol, but they were all legal under Belizean regulations. He alleged that the raid was retaliation for not giving money to politician ahead of general elections last month. McAfee declined to name the politician, saying only that "he was not reelected."

"I am not a man of great stature or anything, why did they have to send over 60 officers to come get me at my compound?" he said.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.